04-01-2026

Fix for the internet

by Stephane van der Aa

Table of contents:

Problems with the internet today 1

The internet is a monopoly 1

There is no authenticity guaranteed 2

Internet core backbone routing is handled by too few Tier1 backbone networks 2

Browser monopoly based on webkit and chromium with Firefox as the fading exception. 3

Solutions 4

Create a transition competitor or competitors for a better global network 4

Authenticity baked in and always tied to a physical person 5

Fishnet topology for better routing 5

New networks will bring new browsers 6

Problems with the internet today

The internet is a monopoly

- There is no competitor to the internet and this has brought innovation to a stand still.
  - Before there the internet became public there were similar privately owned services like Compuserve and America Online. They disappeared with the advent of the internet as the internet quickly overtook them in size making them irrelevant. Yet if they, or others like them would have prevailed there would today be some alternatives. Now we don't get to choose.
- Decisions on "what is supported" get taken by dispirit bodies that do things like introduce IPv6 or abolish protocols like Gopher without clear rational or with a rational that later proves to be invalid.

- IPv6 was supposed to replace IPv4 completely introducing new features allowing more host names and server addresses as IPv4 was going to run out of available addresses, yet today IPv4 still works and there is no shortage of server IP addresses for IPv4 as it turns out. Client IP addresses can be dynamically allocated and reallocated thus solving the problem. As a result the internet is now stuck with 2 addresses for most, one IPv4 requiring 32bits and IPv6 requiring 128bits. For a server supporting both that means its addressing is now 160bits long.
- Gopher was one of the protocols introduced when the internet became open to everyone, next to HTTP, HTML, RSS, FTP,… It is a protocol that allows hierarchical directory browsing. It used to be supported by browsers upon till a few years ago where it was announced that it would no longer be supported on the internet. True it was not used a lot, but there was no technical reason why it had to go. Who takes these decisions and to who are they accountable?

There is no authenticity guaranteed

- Anonymity is impossible in networking, there must always be a source and a destination.
- Today we don't however always know who, what company, what individual is behind the address of the source or destination.
- Over the years it has gotten even worse, supposedly due to data privacy legislation. Protocols like WHOIS that allowed to lookup who owns a domain name, now no longer return useful information. Where before it would return who owns a domain and include contact details of that owner. As a result there is less accountability.
- Cybercrime is allowed to fester because we can no longer determine who is behind an internet address.

Internet core backbone routing is handled by too few Tier1 backbone networks

- The internet is divided in no more then 12 Tier 1 networks that then get used by carriers and eventually ISP's.
- These Tier1 networks are the only places that do the core backbone routing for the entire internet. This is too few technically and in the hands of too few organizations
- This means that packed routing is organized in a hierarchical way whereas a fully distributed architecture would be much more efficient and much more resilient.

Browser monopoly based on webkit and chromium with Firefox as the fading exception.

- Because of the arcane requirements to support a set of technologies to be able to render each web site the world has settled for a quasi browser monopoly based on these 2.
- If the protocols for browsers were better though through and could evolve in a more nimble manor based on sound decisions from a governing body that can introduce innovations but equally important make broadly supported decisions on what protocols and technologies to retire, it would be much easier for someone to create a new browser that does not need to be based on webkit or chromium.
- Chromium by the way is in itself also loosely based on webkit so in reality there really is only one quasi browser type that all internet browsers today are based on.
- Think of what happened to MS Internet Explorer, Netscape and Mosaic, they all were abandoned because they could not keep up ever growing support required to render all websites correctly.
- So more than the fact that there is limited choice in browser engines (Gecko, Blink and Webkit) there is the problem today that to create a new browser not based on one of these 3 becomes simply too much work due to the complexity of what needs to be supported.
- The other problem is that browsers are able to do too much and this creates security issues. Browsers today can detect USB devices, Bluetooth devices and send this information over the internet possibly allowing hackers to take control over much of user's computer by compromising the browser they use. A few decades ago the internet browser was presented as a safe way to connect to the internet because it shielded the user's computer (or device) from the internet only (or mostly only) allowing content to be rendered that was text based (HTML) and that did not interact in a binary way with the rest of the user's computer.

Solutions

Create a transition competitor or competitors for a better global network

This document proposes a radical rethink which will not be something that can be implemented on the current internet as it exists today. As a result a new network needs to emerge. For this to happen there needs to be a transition during which time there this new network will exist alongside the current internet. This transition by itself solves the monopoly of the internet today. Moreover, as the race starts for building a better global network competition should exist from the beginning. Why work towards only one new global network? For the sake of innovation, it would be better if an environment were to exist that lets multiple initiatives for new global networks emerge and grow.

From a user perspective this might seem cumbersome as you either have to choose which global network to use or you need an end user computer or device that supports multiple global networks. This does not need to be such a hind rends. Today on the internet we already see this actually. Websites are typically created for both a desktop and a mobile version. If there were to be multiple global networks most web sites, businesses and organization will simply be made available on these different global networks in order to reach the users. Software development tools will moreover take care of most of the work of supporting multiple global networks in the same way as they help with providing the desktop and mobile versions of web sites today. This will however lead to certain web sites being the first to support all networks and some others taking more time to do so. This in itself is also not a bad thing as it will become fuel for the competition that needs to exist between global networks. Ideally the global network that supports most web sites will change every so often never letting one become the final winner that inevitably renders the laggards obsolete. For this to happen these multiple global networks each need to have key differentiator, so they are not just providing the same functionality, just implemented differently. You can think of such differentiator like having a global network that works well in space with communication throughout our solar system across multiple planets. This multi-planet network will be very different simply due to the limits imposed by the speed of light. Based on the average distance between Earth and Mars for instance it will take 12,5 minutes for a signal (radio, light, …) to arrive. So a global or solar-system network that supports such huge latency would be a key differentiator once our human civilization truly become space faring.

Another key differentiator would be a global network that makes cyber crime as good as impossible by guaranteeing authenticity. But more on that in the next paragraph.

With multiple global networks allowing to compete, they can also compete on the technology stack or protocols they continue to support. Though inherently these

protocols will always be proprietary to the global network. Nonetheless competition should allow on better governance on the technology and protocol stack.

Authenticity baked in and always tied to a physical person

To always be able to have authenticity across a network means not just knowing from which address a request came but also knowing which physical person that address belongs to. When that becomes possible there will clear accountability for all network traffic. Hackers will not dare to hack a web site as their identities will be immediately visible.

How can this work? My idea on this is to create the low level network protocol on the Layer 2 of the OSI model, the link layer, in a way that it includes at that level an identifier of a person. All protocols on the layers above in the OSI model will then inherit that person identifier passing it along through routing and so on. The identifier itself will be issued by a central singular database of identifiers for the whole world. Local country governments may play a role in distributing identifiers. Any human individual can request as many identifiers as he or she wants and these identifiers are then needed to activate any device they use. So you would not be able to use your phone or computer on these new global networks if is not first loaded with such an identifier. These identifiers can also be revoked and thus replaced on devices.

Identifiers would only be assigned to physical persons and not to organization. It will be up to organizations like companies to assign identifiers of the people working for them to for instance servers. This is to make sure there is no possibility where there is a lack of authenticity and accountability. If a person who's identifiers are used for a server of an organization, leaves that organization, than whomever replaces that person must install his or her identifiers on the organization's server to replace those of the person who left.

These identifiers are installed in a way on devices that is directly managed by hardware. We already see today that companies like Apple build in security chips in their devices to do exactly this; securely manage the identifiers of the owner of the devices.

Fishnet topology for better routing

In a fishnet topology a router sits between 4 network connections. These for network connections then either go to the next router or to an end point. Moreover there is no hierarchy between routers. So whoever controls a bunch or routers is not able to carve out a sort of sub net under their control. The routing of traffic happens dynamically based on distance, load on the router and a randomization factor. This means that protocols sending multiple packets for one requests may see these individual packets

follow different routes and thus requiring the destination to handle the rearranging of the arriving packets in the desired order. This will make “eaves dropping” or “wire taping” traffic on a network cable very difficult and impractical. No point of having underwater submarine drones wire tab an underwater fiberoptic cable when what they can intercept in one location on one cable is so fragmented that it becomes nearly impossible to discern the message sent. This fragmentation over the fishnet topology will therefore in effect make such network more secure without even the need for encryption.

New networks will bring new browsers

The problem described with the quasi-browser monopoly today will disappear as new global networks will each come with their own set of protocols requiring completely new browsers. The current browsers may try to support net global networks but they will be doing so without leveraging what makes each global network unique, like getting the most out of the baked-in authenticity. As already explained browsers for such new internet networks will only have to support what is the current and sensible technology and protocol stack which can be better managed thanks to:

- the global network redesign from the ground up
- the ongoing better organization of governing bodies
- the competition between global networks